1963

Projective modules over a group Algebra

George Walter Trickey
The University of Montana

PROJECTIVE MODULES OVER A GROUP ALGEBRA

by

GEORGE WALTER TRICKEY

B.A. Montana State University, 1962

Presented in partial fulfillment of the requirements for

the degree of

Master of Arts

MONTANA STATE UNIVERSITY

1963

Approved by:

William R. Ballard
Chairman, Board of Examiners

Frank C. Abbott
Dean, Graduate School

MAY 31 1963
Date

TABLE OF CONTENTS

INTRODUCTION

In linear algebra and matrix theory the idea of a vector space is basic; recently the more general notion of a module over a ring has come into prominence. One particular type of module is a free module, i. e., vector spaces in the sense that they have a basis. A generalization of the idea of a free module is that of a projective module which in turn has been a powerful tool for the study of linear algebras for modules which are not vector spaces.

The question then arises as to which projective modules are free. The question has been answered satisfactorily in a few elementary cases such as the case where the ring is a local ring. In this case, Kaplansky [3] has shown that every projective module is free. The proof is reproduced in Chapter One. When the ring is more general, the question has remained unanswered. Swan [6] has done much work along this line in the case of a group ring where the ring is a Dedekind domain. He shows that a projective module in this case is the direct sum of a free module and a projective ideal in the group ring. The more interesting part of his paper is contained in Chapter Two.

CHAPTER 0.

SOME PRELIMINARY RESULTS.

Let R be a ring with identity. Let M be an abelian additive group. M is called a <u>left R-module</u> if for each element x of M and each element r of R, there is defined a product rx which belongs to M and satisfies the following axioms:

i) $r(x + y) = rx + ry$

ii) $(r + s)x = rx + sx$

iii) $r(sx) = (rs)x$

iv) $1x = x$

where x and y are arbitrary elements of M, and r and s are arbitrary elements of R. The identity of the ring is denoted by 1.

We may define <u>right R-modules</u> in a symmetric manner. We will use left R-modules throughout the paper many times without designation. Any result which holds for left modules will also hold for right modules with very little change in proof.

If M is a R-module, and N is a subgroup of M then N is a <u>R-submodule</u> in case $rn \in N$ for all $n \in N$ and $r \in R$. Let M be a R-module and N a submodule of M. The <u>difference</u> or <u>quotient module</u> M/N is the R-module whose group is the family of cosets $\{m + N\}$, $m \in M$, with module composition defined by

$$r(m + N) = rm + N.$$

The addition is well-defined since N is a R-submodule of M.

Let $\{M_i\}$ be a possibly infinite family of submodules of M. The sum ΣM_i of the family is the submodule whose elements are all possible finite sums of elements from the various M_i.

If we have a mapping from M into N we write $f : M \to N$ or

$$M \xrightarrow{f} N.$$

If M and N are R-modules, we say f is a homomorphism in case it is a group homomorphism, i.e.,

$$f(x + y) = f(x) + f(y) \qquad \text{for } x \text{ and } y \text{ in } M.$$

We say that f is a R-homomorphism if in addition it satisfies

$$f(rx) = rf(x) \qquad \text{for all } r \in R \text{ and } x \in M.$$

Let $f : M \to N$ and $g : N \to Q$ be homomorphisms where M, N and Q are R-modules. We define $gf : M \to Q$ by

$$gf(x) = g(f(x)) \qquad \text{for } x \in M.$$

If we have a diagram of modules and homomorphisms

$$\begin{tikzcd}
M_1 \arrow[r, "f_1"] \arrow[d, "g_1"'] & M_2 \arrow[r, "f_2"] & \cdots \arrow[r, "f_{n-1}"] & M_n \arrow[d, "f_n"] \\
N_1 \arrow[r, "g_2"] & N_2 \arrow[r, "g_3"] & \cdots \arrow[r, "g_n"] & N_n
\end{tikzcd}$$

and $f_n f_{n-1} \cdots f_1 = g_n g_{n-1} \cdots g_1$ then we say that the diagram is commutative.

f is said to be injective or a monomorphism if it is 1-1, surjective or an epimorphism if it is onto, and bijective or an isomorphism if it is 1-1 and onto.

We further define:

Ker f (kernel of f)	is	$\{x: f(x) = 0\}$, which is a submodule of M;
Im f (image of f)	is	$\{f(x): x \in M\}$, which is a submodule of N;
Coker f (cokernel of f)	is	$N/\text{Im } f$; and
Coim f (coimage of f)	is	$M/\text{Ker } f$.

A sequence of homomorphisms

$$\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

is called <u>exact</u> if $\text{Ker } f_i = \text{Im } f_{i-1}$ for each i.

Suppose M' is a submodule of M. Then

$$0 \to M' \to M \to M/M' \to 0$$

is exact, where 0 is the zero-module, $M' \to M$ is the inclusion map and $M \to M/M'$ is the canonical map defined by $f(m) = m + M'$.

Let us denote the set of all R-homomorphisms from M into N by $\text{Hom}_R(M, N)$. $\text{Hom}_R(M, N)$ is a group with addition defined by

$$(f + g)(m) = f(m) + g(m)$$

for $m \in M$ and $f, g \in \text{Hom}_R(M, N)$.

If $f : M' \to M$ and $g : N \to N'$ are R-homomorphisms we have a homomorphism

$$\text{Hom}_R(f, g) : \text{Hom}_R(M, N) \to \text{Hom}_R(M', N')$$

defined by

$$\text{Hom}_R(f, g)(h) = ghf.$$

We have the diagram

$$\begin{tikzcd} M' & M \arrow[l, "f"'] \arrow[d, "h"] \\ N' & N \arrow[l, "g"] \end{tikzcd}$$

Let $\{M_\alpha\}$, $\alpha \in I$ where I is some index set, be a family of R-modules. Let

$$M = \prod_\alpha M_\alpha \quad \text{(Cartesian product of the } M_\alpha\text{'s as sets).}$$

M is a R-module if we define addition and multiplication (by elements of R) in co-ordinate-wise fashion, i.e.,

$$[m_\alpha] + [n_\alpha] = (. \; . \; ., m_\alpha, \; . \; . \; .) + (. \; . \; ., n_\alpha, \; . \; . \; .)$$
$$= (. \; . \; ., m_\alpha + n_\alpha, \; . \; . \; .)$$

where $m_\alpha \in M_\alpha$, $n_\alpha \in N_\alpha$. We have co-ordinate projections $p_\alpha : M \to M_\alpha$, $\alpha \in I$, and we see that each p_α is an epimorphism. If

$$f : N \to M$$

is any homomorphism, then $\{p_\alpha f\}$, $\alpha \in I$, is a family of homomorphisms making the diagrams

$$\begin{tikzcd} M \arrow[r, "p_\alpha"] & M_\alpha \\ N \arrow[u, "f"] \arrow[ur, "p_\alpha f"'] & \end{tikzcd}$$

commutative.

Conversely, given a family $\{f_\alpha\}$ such that $f_\alpha : N \to M_\alpha$ there exists a unique $f : N \to M$ making all triangles

$$\begin{tikzcd} N \arrow[r, "f_\alpha"] \arrow[d, "f"'] & M_\alpha \\ M \arrow[ur, "p_\alpha"'] & \end{tikzcd}$$

commutative diagrams, i. e.,

$$f(x) = [f_\alpha(x)] \in M = \prod_\alpha M_\alpha.$$

A direct product of $\{M_\alpha\}$, $\alpha \in I$, is a module M together with homomorphisms $p_\alpha : M \to M_\alpha$, such that for each N the mapping

$$\mathrm{Hom}_R\,(N, M) \to \prod_\alpha \mathrm{Hom}_R\,(N, M_\alpha)$$

given by

$$f \to (.\ .\ ., p_\alpha f, .\ .\ .)$$

is bijective.

Let us consider $M = \prod_\alpha M_\alpha$, as above. We also have a family of injection maps $\{i_\alpha\}$, $i_\alpha : M_\alpha \to M$. Each i_α is clearly a monomorphism. If $f : M \to N$ is any homomorphism, $\{fi_\alpha\}$, $\alpha \in I$, is a family of homomorphisms making the triangles

$$\begin{tikzcd} M_\alpha \arrow[d, "i_\alpha"'] \arrow[dr, "fi_\alpha"] & \\ M \arrow[r, "f"] & N \end{tikzcd}$$

commutative.

Conversely, given a family $\{f_\alpha\}$, $\alpha \in I$, of homomorphisms

$$f_\alpha : M_\alpha \to N,$$

there exists a unique homomorphism $f : M \to N$ making all triangles

$$\begin{tikzcd}
M \arrow[dr, "f"] & \\
M_\alpha \arrow[u, "i_\alpha"] \arrow[r, "f\alpha"'] & N
\end{tikzcd}$$

commutative diagrams.

A <u>direct sum</u> of $\{M_\alpha\}$, $\alpha \in I$, is a module M together with homomorphisms $I_\alpha : M_\alpha \to M$ such that for each N the mapping

$$\mathrm{Hom}_R\,(M,\ N) \to \prod_\alpha \mathrm{Hom}_R\,(M_\alpha,\ N)$$

given by

$$f \quad \to \quad fi_\alpha$$

is bijective.

If we denote the product by $\prod\limits_\alpha M_\alpha$ and the direct sum by $\bigoplus\limits_\alpha M_\alpha$ then the definition may be abbreviated

$$\mathrm{Hom}_R\,(N,\ \prod_\alpha M_\alpha) = \prod_\alpha \mathrm{Hom}_R\,(N,\ M_\alpha)$$

$$\mathrm{Hom}_R\,(\ \bigoplus M_\alpha,\ N) = \prod_\alpha \mathrm{Hom}_R\,(M_\alpha,\ N).$$

Assume that $M = \bigoplus M_\alpha$ and $N = \bigoplus M_\alpha$, $\alpha \in I$. Let us consider the diagram

$$\begin{tikzcd}
N \arrow[r, "f"] & M \arrow[r, "g"] & N \\
& M_\alpha \arrow[ul, "i_\alpha"] \arrow[u, "i_\alpha"] \arrow[ur, "i_\alpha"'] &
\end{tikzcd}$$

The triangles are commutative for all homomorphisms, f and g, by the remark above. Hence the diagram

$$\begin{tikzcd} M \arrow[rr, "fg"] & & M \\ & M_\alpha \arrow[ul, "i_\alpha"] \arrow[ur, "i_\alpha"'] & \end{tikzcd}$$

must be commutative. We now have by the uniqueness that gf = identity homomorphism $1_M : M \to M$.

If we repeat the argument on

$$\begin{tikzcd} N \arrow[r, "g"] & M \arrow[r, "f"] & N \\ & M_\alpha \arrow[ul, "i_\alpha"] \arrow[u, "i_\alpha"] \arrow[ur, "i_\alpha"'] & \end{tikzcd}$$

we see that fg = identity map $1_N : N \to N$, and we have that M and N are isomorphic.

Let N' be the submodule of $\prod_\alpha M_\alpha$ consisting of all vectors $\{x_\alpha\}$ such that $x_\alpha = 0$ for all but a finite number of the α's. Define

$$i_\alpha : M_\alpha \to N'$$

by

$$i_\alpha(x) = (x_\beta), \qquad x \in M_\alpha,$$

where $x_\beta = x$ if $\alpha = \beta$ and $x_\beta = 0$, otherwise. We see then that N' is a direct sum.

Proposition 0.1. If $M_1, M_2, \ldots, M_n$ are R-modules, an R-module M is isomorphic to a direct sum of $M_1, M_2, \ldots, M_n$ if and only if there exist $i_\alpha : M_\alpha \to M$ and $p_\alpha : M \to M_\alpha$ such that

1) $p_\alpha i_\beta = 0$ if $\alpha \neq \beta$, $p_\alpha i_\alpha = 1_{M_\alpha}$, $p_\alpha i_\alpha(x) = x$ for all x.

2) $\Sigma\, i_\alpha p_\alpha = 1_M$; $\Sigma\, i_\alpha p_\alpha(x) = x$ for all x, where 1_M, 1_{M_α} denote the identity maps on M and M_α, respectively.

PROOF: Let M' be as in the remark above. Clearly there exist $\{i_\alpha\}$ and $\{p_\alpha\}$ with the desired properties.

Suppose then, that (1) and (2) hold and consider the homomorphism

$$f : \prod_\alpha M_\alpha \to M$$

defined by

$$f[m_\alpha] = \Sigma\, i_\alpha(m_\alpha), \qquad m_\alpha \in M_\alpha.$$

If $\sum_{\alpha=1}^{n} i_\alpha(m_\alpha) = 0$, then $0 = p_\beta(\Sigma\, i_\alpha(m_\alpha)) = m_\beta$ for all β so $\prod_{\alpha=1}^{n} M_\alpha \to M$ is a monomorphism. Let $m \in M$. Then $\sum_{\alpha=1}^{n} i_\alpha p_\alpha(m) = m$. $[p_\alpha(m)] \in \Pi\, M_\alpha$, and by (2), its image in M is $\sum_{\alpha=1}^{n} i_\alpha p_\alpha(m) = m$. So $\prod_{\alpha=1}^{n} M_\alpha \to M$ is an isomorphism. The remark shows that in this case, however,

$$\prod_{\alpha=1}^{n} M_\alpha \cong \bigoplus_{\alpha=1}^{n} M_\alpha \qquad (\text{"}\cong\text{" means "is isomorphic to"}).$$

Theorem 0.2. Let $M = M_1 \oplus M_2 \oplus M_3 \oplus \cdot\cdot\cdot \oplus M_r$. Let N_i be a submodule of M_i ($i = 1, 2, \ldots, r$) and let $N = N_1 + N_2 + \cdot\cdot\cdot + N_r$. Then this sum is direct and M/N is a direct sum of submodules R-isomorphic to the difference modules M_i/N_i.

PROOF: That $N \cong N_1 \oplus N_2 \oplus \cdot\cdot\cdot \oplus N_r$ is evidant; i.e., $\mathrm{Hom}_R\,(N, Q) \to \prod_{\alpha=1}^{n} \mathrm{Hom}_R\,(N_\alpha, Q)$ is bijective for all Q. (Consider maps restricted to N).

Let f be the canonical map

$$f : M \to M/N.$$

To show that $f(M) \cong \oplus\, f(M_\alpha)$ it is sufficient to show that there exist $[p_\alpha]$ and $[i_\alpha]$ with the properties in Theorem 0.1.

Consider the diagram

$$\begin{tikzcd} M_\alpha \arrow[r, "i_\alpha"] \arrow[d, "f"] & M \arrow[r, "p_\alpha"] \arrow[d, "f"] & M_\alpha \arrow[d] \\ f(M_\alpha) \arrow[r, "g_\alpha"] & f(M) \arrow[r, "h_\alpha"] & f(M_\alpha) \end{tikzcd}$$

Each square is commutative, i.e., $fi_\alpha = g_\alpha f$ and $fp_\alpha = h_\alpha f$. We claim $\{g_\alpha\}$ and $\{h_\alpha\}$ will have the properties required.

$$1)\ h_\alpha g_\alpha(f(m_\alpha)) = h_\alpha(g_\alpha f(m_\alpha)) = h_\alpha(fi_\alpha(m_\alpha))$$

$$= h_\alpha f(i_\alpha(m_\alpha)) = f(p_\alpha i_\alpha(m_\alpha)) = f(m_\alpha), \text{ and}$$

$$h_\beta g_\alpha(f(m_\alpha)) = f(0) = 0 \qquad\qquad \text{if } \beta \neq \alpha.$$

$$2)\ \sum_{\alpha=1}^{n} g_\alpha h_\alpha(f(m)) = \sum_{\alpha=1}^{n} g_\alpha f(p_\alpha(m)) = \sum_{\alpha=1}^{n} f(i_\alpha p_\alpha(m))$$

$$= f \sum_{\alpha=1}^{n} i_\alpha p_\alpha(m) = f(m).$$

It remains to show that $f(M_i) \cong M_i/N_i$. This follows since $M_i \cap N = N_i$ implies that f restricted to M_i has N_i as kernel.

We call a module P projective if given a diagram

$$\begin{tikzcd} & P \arrow[d, "f"] & \\ M \arrow[r, "g"] & N \arrow[r] & 0 \end{tikzcd}$$

with the bottom row exact, there exists $\phi : P \to M$ such that $g\,\phi = f$; in other words, the diagram

$$\begin{tikzcd} & P \arrow[d, "f"] \arrow[dl, "\phi"'] & \\ M \arrow[r, "g"] & N \arrow[r] & 0 \end{tikzcd}$$

is commutative.

A collection $\{u_i\}$, $i \in I$, of elements of a R-module M is a set of generators in case, for each $x \in M$

$$x = \Sigma\, r_i u_i$$

where each $r_i \in R$ and only finitely many r_i's $\neq 0$.

If for each element x of M, the r_i's for which

$$x = \sum_j r_j u_j$$

are uniquely determined, then $\{u_i\}$ is called a base for M. A module which admits a base is called free.

Theorem 0.3. Let M be any R-module. There exists a free R-module F with an epimorphism $F \to M$. If M has n generators $(0 \leq n < \infty)$ then F can be chosen with a base of n elements.

PROOF: Let $\{u_i\}$, $i \in I$, be a system of generators of M. Let $\{v_i\}$, $i \in I$, be a system of distinct elements similarly indexed. Let F be the set of all formal sums, $\sum_i r_i v_i$, where each $v_i \in R$ and $r_i = 0$ for all but a finite number of the i's. Let us identify v_i with $\Sigma\, \delta_{ij} v_i$ where

$$\delta_{ii} = 1 \qquad \text{and} \qquad \delta_{ij} = 0, \qquad i \neq j.$$

Then if we define addition and multiplication (by elements of R) of the formal sums in the obvious manner we see that F is a free R-module with $\{v_i\}$ as a base. Let

$$f : F \to M$$

be defined by

$$f(\Sigma\, r_i v_i) = \Sigma\, r_i u_i$$

f clearly is a homomorphism and will do the job.

Let F be a free module with base $\{v_i\}$, $i \in I$. Let M be a R-module and let $\{u_i\}$, $i \in I$, be a family of elements of M. There always exists a unique homomorphism $f : F \to M$ such that

$$f(v_i) = u_i.$$

In fact, we define f by

$$f(\sum_i r_i v_i) = \sum r_i u_i.$$

Theorem 0.4. Let F be a free R-module, $p : F \to N$ an R-homomorphism, and $q : M \to N$ an epimorphism of R-modules. Then there exists an R-homomorphism $\phi : F \to M$ such that $\phi q = p$, i.e., the diagram

$$\begin{tikzcd} & F \arrow[dl, "\phi"'] \arrow[d, "p"] & \\ M \arrow[r, "q"] & N \arrow[r] & 0 \end{tikzcd}$$

is commutative.

PROOF: Let $\{u_i\}$, i.e., I, be a base for F. Then $p(u_i) \in N$ for each i. Since q is an epimorphism there exists an element $v_i \in M$ such that $q(v_i) = p(u_i)$. F is free so there exists a homomorphism $\phi : F \to M$ such that $\phi(u_i) = v_i$. Then

$$q\phi(u_i) = q(v_i) = p(u_i).$$

we have that $q\phi$ and p agree on a basis of F and hence on all elements of F.

Proposition 0.5. A direct sum $M = \oplus M_\alpha$, $\alpha \in I$, of R-modules is R-projective if and only if each M_α is R-projective.

PROOF: Assume $M \cong N \oplus M_\alpha$ where M is projective. Consider the diagram

$$\begin{array}{ccccccc} M_\alpha & \xrightarrow{i_\alpha} & M & \xrightarrow{p_\alpha} & M_\alpha & & \\ & & h\downarrow & & f\downarrow & & \\ & & A & \xrightarrow{g} & B & \to & 0 \end{array}$$

where the bottom row is exact, and p_α and i_α are the projection map and injection map, respectively. Now there exists a map

$$h : M \to A$$

such that

$$gh = fp_\alpha.$$

Then hi_α is the desired map.

Assume each M_α is projective. Then consider the diagram

$$\begin{array}{ccccccc} M & \xrightarrow{p_\alpha} & M_\alpha & \xrightarrow{i_\alpha} & M & & \\ & & h\downarrow & & f\downarrow & & \\ & & A & \xrightarrow{g} & B & \to & 0 \end{array}$$

with the bottom row exact. It is clear then that $\Sigma\, hp_\alpha$ will do the job.

There is a close connection between projective and free modules as illustrated by

Theorem 0.6. Let M be a R-module. Then M is projective if and only if M is a direct summand of a free R-module.

PROOF: We will first show that if M is projective then M is a direct summand of a free R-module. By Theorem 0.4 there exists a

R-free module F such that $p : F \to M$ is an epimorphism. Let K be Ker p, and consider the diagram

$$(*) \qquad 0 \to K \xrightarrow{f} F \xrightarrow{p} M \to 0$$

M is projective so there exists a map $q : M \to F$, such that $pq = 1_M$. Let $m \in F$ and let

$$qp(m) = a$$

where $a \in q(M)$. Then

$$p(m - a) = p(m) - pq(p(m)) = 0.$$

Therefore, $m - a = b$, where $b \in K$, or $m = a + b$. Define $g(m) = b$. Then

$$g : F \to K.$$

To show that $F = M \oplus K$, it will suffice, by Proposition 0.1, to show that

1) $qp + fg = 1_F$

2) $pf = gq = 0$.

We have that

$$(qp + fg)(a + b) = a + b.$$

To show that condition (2) is satisfied, we note first that $pf = 0$, since $(*)$ is exact. Let $a \in M$; then $gq(m) = g(a) = 0$. Thus $gq = 0$.

To show that a direct summand of a free module is projective we recall that a free module is projective by Theorem 0.4. Then by Theorem 0.5, a direct summand of a projective module is projective.

Let M be a left R-module and N be a right R-module. As usual we are assuming that R has an identity. Let P be an abelian group, written additively. A <u>balanced map</u> f of the Cartesian product $M \times N$ into P assigns to each pair (m, n) in $M \times N$ an element $f(m, n)$ in P, such that

$$f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n),$$
$$f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2),$$

and

$$f(m, rn) \qquad = f(mr, n),$$

whenever $m_1, m_2, m \in M$ and $r \in R$.

Suppose that $f : M \times N \to P$ and $\varphi : M \times N \to T$ are balanced maps into the additive abelian groups P and T respectively. We say that f can be <u>factored through</u> T if there exists a homomorphism $f^* : T \to P$ such that

$$f = f^*\varphi,$$

or, to be explicit,

$$f(m, n) = f^*(\varphi(m, n))$$

for all (m, n) in $M \times N$. The diagram

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi} & T \\ & \searrow^{f} & \downarrow f^* \\ & & P \end{array}$$

is commutative.

Theorem 0.7. Let M and N be right and left R-modules, respectively. There exists an abelian group T and a balanced map $f : M \times N \to T$ such that

1) the elements $f(m, n)$ generate the group T and, in fact, every element of T is a finite sum $\sum_i f(m_i, n_i)$, $m_i \in M$, $n_i \in N$.

2) Every balanced map of $M \times N$ into an arbitrary abelian group P can be factored through T in a unique fashion.

T will be called the tensor product of M and N, denoted $M \otimes_R N$.

PROOF: For the proof of the existence of the tensor product see, for example, Curtis and Reiner [2; 12.3].

We will assume the following properties of the tensor product:

i) Associativity: $(M \otimes_R N) \otimes_R Q \cong M \otimes_R (N \otimes_R Q)$

ii) Commutativity: $M \otimes_R N \cong N \otimes_R M$; and

iii) Distributivity: $(\bigoplus_i M_i) \otimes_R N \cong \bigoplus_i (M_i \otimes_R N)$, and

$M \otimes_R (\bigoplus N_i) \cong \bigoplus_i (M \otimes_R N_i)$

Theorem 0.8. Let $f : M \to M'$ and $g : N \to N'$ be R-homomorphisms, where M and M' are right R-modules and N and N' are left R-modules. Then there exists a unique homomorphism

$$f \otimes g : M \otimes N \to M' \otimes N'$$

such that

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$

PROOF: The map $(m, n) \to f(m) \otimes g(n)$ is balanced. The existence and uniqueness now follow immediately from Theorem 0.7.

We will be interested in exact sequences and when the exactness will be preserved under the operations. We find that tensoring with a module will preserve exactness on the right, in general.

Theorem 0.9. If $M' \xrightarrow{f'} M \xrightarrow{f} M'' \to 0$ is an exact sequence of right R-modules then, for every left R-module N,

$$M' \otimes N \xrightarrow{f'\otimes 1_N} M \otimes N \xrightarrow{f\otimes 1_N} M'' \otimes N \to 0$$

is exact. We can interchange left and right and the theorem will still hold.

PROOF: $(f \otimes 1_N)(f' \otimes 1_N) = (ff' \otimes 1_N) = 0 \otimes 1_N = 0$. Therefore we have Im $(f' \otimes 1_N)$ is contained in Ker $(f \otimes 1_N)$ and $(f \otimes 1_N)(\mathrm{Im}\,(f' \otimes 1_N)) = 0$. Thus $f \otimes 1_N$ induces a map

$$u : \mathrm{Coker}\,(f' \otimes 1_N) \to M'' \otimes N,$$

with

$$\mathrm{Ker}\; u = \mathrm{Ker}\,(f \otimes 1_N)/\mathrm{Im}\,(f' \otimes 1_N).$$

For exactness, it remains only to show that u is an isomorphism. We will show this by constructing the inverse v.

Given $m'' \otimes n$, define $v(m'' \otimes n)$ by choosing $m \in M$ such that $f(m) = m''$, (this we may do by the exactness), and letting $v(m'' \otimes n) =$ coset of $m \otimes n$ in Coker $(f' \otimes 1)$. Suppose m_1 is a second choice, i.e., $f''(m_1) = m''$. Then $f''(m - m_1) = 0$ so $m - m_1$ is in Ker f'' = Im f' (by the exactness). Therefore $m = m' + f'(m')$ for some $m' \in M'$ and

$$m \otimes n = (m_1 + f'(m')) \otimes n = (m_1 \otimes n) + (f'(m') \otimes n)$$
$$= (m_1 \otimes n) + (f' \otimes 1)(m' \otimes n).$$

So we have

$$\text{coset } m \otimes n = \text{coset } m_1 \otimes n$$

relative to Im $(f' \otimes 1_N)$.

If $f(m) = m''$ and $f(m_1) = m_1''$ then $f(m) + f(m_1) = m'' + m_1''$. Therefore, $v((m'' + m_1'') \otimes n) =$ coset $(m + m_1) \otimes n_1$

$$= \text{coset } [(m \otimes n) + (m_1 \otimes n)].$$

If $f'(m) = m''$ and $a \in R$, then $f(ma) = f(m)a = m''a$, so $v(m''a \otimes n) =$ coset $(ma \otimes n) =$ coset $m \otimes an = v(m'' \otimes an)$. Now $vu(\text{coset } m \otimes n) = v(f''(m) \otimes n) = \text{coset } m \otimes n$ and $uv(m'' \otimes n) = u(\text{coset } m \otimes n) = f''(m \otimes n) = m'' \otimes n$ when $f''(m) = m''$. Thus v is the desired inverse.

Theorem 0.10. Let R be a ring and N a left R-module. Then $R \otimes_R N \cong N$.

PROOF: The map $(r, n) \to rn$ is a balanced map of $R \otimes N$ into N, and so by Theorem 0.2 there exists a homomorphism $f : R \otimes_R N \to N$ such that $f(r \otimes n) = rn$. On the other hand we may define a map $g : N \to R \otimes_R N$ by

$$g(n) = 1 \otimes n, \qquad n \text{ in } N.$$

Clearly fg acts as the identity map on N; furthermore,

$$gf(r \otimes n) = g(rn) = 1 \otimes rn = r \otimes n,$$

so gf acts as the identity map on $R \otimes_R N$. That f is an R-isomorphism of left R-modules is clear.

Corollary 0.11. Let I be a right ideal in a ring R. Let M be a left R-module. Then

$$M/IM \cong R/I \otimes_R M.$$

PROOF: $0 \to I \xrightarrow{i} R \to R/I \to 0$ is exact. By Theorem 0.9 then we have

$$I \otimes_R M \to R \otimes_R M \to R/I \otimes_R M \to 0$$

is exact. We have that $R \otimes_R M \cong M$, so

$$R/I \otimes_R M \cong M/\text{Im } (I \otimes_R M).$$

$\text{Im } (I \otimes_R M = \{\Sigma\, r_i m_i ; r_i \in I\} = IM$, and this then gives the desired result.

Let H be any finite group. Then we can build a group ring from R, denoted RH, by considering all formal sums

$$\Sigma\ \alpha_g g \qquad \text{where } g \in H,\ \alpha_g \in R.$$

We define operations on the formal sums by the rules

$$\sum_{g\in H} \alpha_g g + \sum_{g\in H} \beta_g g = \sum_{g\in H} (\alpha_g + \beta_g) g$$

and

$$\Big(\sum_{g\in H} \alpha_g g\Big)\Big(\sum_{g\in H} \beta_h h\Big) = \sum_{g\in H} \alpha_g \beta_h gh = \sum_{t\in H} \gamma_t t$$

where

$$\gamma_t = \Sigma\ \alpha_g \beta_{g^{-1}t}$$

If A and B are RH-modules we define $A \otimes B$ by $A \otimes_R B$ as R-modules with H-action defined by $g(A \otimes B) = gA \otimes gB$, $g \in H$.

Let K be the field of quotients of R. Let M be a left R-module with set of generators $\{m_i\}$, i in some index set. $\{1 \otimes m_i\}$ is a system of generators for $K \otimes_R M$ and it is easy to verify that the system forms a basis for $K \otimes_R M$ as a vector space over K. The R-rank for M, denoted rk M, is the dimension, $(K \otimes_R M : K)$, of $K \otimes_R M$ as a vector space over K.

CHAPTER I.

MODULES OVER A LOCAL RING.

By a <u>local ring</u> we mean a commutative ring in which the non-units form an ideal. In this chapter we will give the proof that a projective module over a local ring is free. Kaplansky gives the original proof which we use [3]. The result is well known in the case that the projective module is finitely generated [1]. The proof in the general case requires a surprising result of Kaplansky which we now give.

Theorem 1.1. Let R be an arbitrary ring with identity and M an R-module which is a direct sum of countably generated R-modules. Then any direct summand of M is a direct sum of countably generated R-modules.

PROOF: Let $M = \bigoplus_i M_i$, where each M_i is countably generated. Suppose $M = P \oplus Q$. To prove P is a direct sum of countably generated modules, we will express M as a union of a well-ordered sequence of submodules $\{S_\alpha\}$ with the properties:

1) if α is a limit ordinal, $S_\alpha = \bigcup_{\beta<\alpha} S_\beta$.

2) $S_{\alpha+1}/S_\alpha$ is countably generated.

3) each S_α is the direct sum of a subset of the M_i's.

4) $S_\alpha = P_\alpha \oplus Q_\alpha$, where $P_\alpha = S_\alpha \cap P$, $Q_\alpha = S_\alpha \cap Q$.

Assume that this has been done and we will see that this will suffice.

We have then that P_α is a direct summand of S_α, which is a direct summand of M. So P_α is a direct summand of M and, by the properties of the S_α's, is a direct summand of $P_{\alpha+1}$. Since, by Theorem 0.2,

$$S_{\alpha+1}/S_\alpha \cong P_{\alpha+1}/P_\alpha \oplus Q_{\alpha+1}/Q_\alpha,$$

$P_{\alpha+1}/P_\alpha$ is a countably generated module. It is clear that, if α is a limit ordinal, $P_\alpha = \bigcup_{\beta<\alpha} P_\beta$. Thus we have

$$P_{\alpha+1} = P_\alpha \oplus P_\alpha',$$

where P_α' is countably generated, since it is isomorphic to $P_{\alpha+1}/P_\alpha$. Now, $\oplus P_\alpha' \cong M \cap P \cong P$ and this is what we need.

In order to construct S_α we have no trouble if α is a limit ordinal. Assume that S_α is at hand for some ordinal α. We will now procede to construct an infinite matrix which we will use to define $S_{\alpha+1}$. If $S_\alpha = M$, we have finished; hence, suppose $S_\alpha \neq M$. Choose some M_j which is not contained in S_α. Let $\{x_{1n}\}$, $n = 1, 2, \ldots$, be a countable generating set for M_j. This is the first row of our matrix. Split x_{11} into its P- and Q-components. Each of these new elements in the expression of M as a direct sum of the M_i's, has a non-zero entry in only a finite number of the M_i's. Take this finite collection of the M_i's and let $\{x_{2n}\}$ denote a countable set of generators for their union. This is the second row. Next repeat the process on x_{12} that was applied to x_{11}. The result will be the third row of the infinite matrix we are building. Continue in this fashion, pursuing the elements along successive diagonals in the order, $x_{11}, x_{12}, x_{21}, x_{12}, \ldots$. $S_{\alpha+1}$ is taken to be the submodule generated by S_α and all the x_{ik}'s. We see readily that (1) through (4) are satisfied by $S_{\alpha+1}$.

Theorem 1.2. A projective module over a local ring is free. We will break the proof into two lemmas.

Lemma 1.3. Let R be any ring and M a countably generated R-module. Assume that any direct summand N of M has the property that any element of N can be embedded in a free (respectively, finitely generated) direct summand of N. Then M is free (resp., a direct sum of finitely generated modules).

PROOF: Write $M = P_1 \oplus Q_1$. If P_1 or Q_1 is trivial we are done. Assume then that this is not the case. Let x_1 be a generator for M. Let x_{11} and y_{11} be its P_1- and Q_1-components, respectively. Then x_{11} can be embedded in a free (finitely generated) direct summand F_1 of P_1. Similarly, y_{11} can be embedded in G_1, say. If P_1 or Q_1 has no free (finitely generated) direct summand, then it must be free (finitely generated). If this is not the case then

$$M = P_2 \oplus F_1 \oplus Q_2 \oplus G_1 = P_2 \oplus Q_2 \oplus H_2$$

where $P_1 = P_2 \oplus F_1$, $Q_1 = Q_2 \oplus G_1$ and H_2 is free (finitely generated). Let x_2 be another generator for M. Let x_{21}, y_{21}, f_2 be its P_2, Q_2, and H_2-components, respectively. We can embed x_{21} and y_{21} in free (finitely generated) direct summands, F_2 and G_2, of P_2 and Q_2, respectively. In the case that P_2 or Q_2 has no free (finitely generated) direct summand it is itself free (finitely generated). We see that this process can be continued and hence we can embed all generators of M in a direct sum of free (finitely generated)submodules. Thus M is isomorphic to a direct sum of free (finitely generated) modules and hence is free.

Lemma 1.4. Let P be a projective module over a local ring. Then any element of P can be embedded in a free direct summand of P.

PROOF: Write $F = P \oplus Q$, where F is free. Let $x \in P$. Select a basis $\{u_i\}$ of F such that $x = \sum_{i=1}^{n} a_i u_i$ and n is the smallest number of terms possible. None of the a_i's can be a right linear combination of the remaining ones. For suppose $a_n = a_1 b_1 + \ldots + a_{n-1} b_{n-1}$. If we replace u_i by $u_i + b_i u_n$, $i = 1, 2, \ldots, n-1$, and leave all other basis elements unchanged, we get a new basis for F. Thus,

$$x = a_1(u_1 + b_1 u_n) + \ldots + a_{n-1}(u_{n-1} + b_{n-1} u_n)$$

is a shorter expression for x, contradicting the choice of n.

Let $u_i = y_i + z_i$ be a decomposition of u_i into P- and Q-components, $i = 1, 2, \ldots, n$. Then necessarily

(1) $$\sum a_i y_i = \sum a_i u_i \qquad i = 1, 2, \ldots, n$$

since each is the P-component of x. Write $y_i = \sum c_{ij} u_j + t_i$ where t_i is a linear combination of the basis elements other than u_i, $i = 1, 2, \ldots, n$. Combine this with (1) and equate coefficients of u_j. Then

$$a_1 c_{1j} + a_2 c_{2j} + \ldots + a_n c_{nj} = a_j.$$

Now $c_{jj} - 1$ and c_{ij}, $i \neq j$, must be non-units; otherwise some a_i would be a right linear combination of the others which we have seen is impossible. Hence the matrix (c_{ij}) is non-singular; for it has units down the main diagonal and non-units elsewhere, and over a local ring this is sufficient to make it non-singular. To see this, let (c_{ij}) be a matrix over a local ring with units down the main diagonal and non-units elsewhere. The determinant, $|c_{ij}|$, of (c_{ij}) is equal to $m_i + \Sigma n_i$, m_i a unit in the local ring and each n_i a product of non-units, then $m_i + \Sigma n_i$ must be a unit since the non-units form an ideal, and Σn_i is a non-unit. Thus $y_1, y_2, \ldots, y_n$ form a basis for F when augmented by the u's other than $u_1, u_2, \ldots, u_n$. If we write S for the submodule generated by the y_i's, we have $x \in S \subseteq P$. Since S is a free direct summand of F, S is a free direct summand of P. To see this, we note first that we can write

$$M = S \oplus R$$

where R is a submodule of Q; hence, M is a submodule of F.

Consider the diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & R & \to & Q & \to & Q/R & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & M & \to & F & \to & F/M & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & S & \to & P & \to & P/S & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where each row and column is exact. The exactness of the third column follows by Theorem 0.2. Using the properties of direct sums we see that there is a map from P/S to P, by mapping P/S to F/M first, and then mapping F/M to F. Similarly, there is a map from P to S. These maps clearly will satisfy the conditions required.

To prove Theorem 1.2 is now an easy job. A projective module is a direct summand of a free module. A free module can be written as a direct sum of countably generated modules; therefore, by Theorem 1.1 a projective module is a direct sum of countably generated modules, each of which is necessarily projective. By Lemma 1.4, we can embed any element of a projective module P in a free direct summand of P. Now we apply Lemma 1.3. We now see that a projective module can then be written as a direct sum of free modules, which is what was needed.

We will require one more theorem for later chapters which would seem to belong in this chapter. The proof will be omitted but may be found in [2; 77] or [5; 1]. We state the theorem:

Theorem A. Let R be a local ring and K its field of quotients. Let H be any finite group. If M and N are projective RH-modules, then M is isomorphic to N whenever $K \otimes M$ is isomorphic to $K \otimes N$.

The theorem would require proof of the non-singularity of the "Cartan" matrix. Curtis and Reiner give a proof which requires considerable background in the theory of group characters while Swan uses the "Artin" induction theorem generalized to "Groethendieck" rings to prove the theorem. Either of these proofs would lead us far from the path we are following.

CHAPTER II.

MODULES OVER A DEDEKIND RING.

We are concerned with Noetherian domains (every ascending chain of ideals terminates) with the property that every ideal is projective. Such rings are called <u>Dedekind rings.</u> The usual definition states that R is a Dedekind domain if and only if it is a Noetherian domain with the property that each ideal I is invertible, i.e., that there exist $q_1, q_2, \ldots, q_n$ in the field of quotients, K, of R and $a_1, a_2, \ldots, a_n$ in I with q_iI contained in R and

$$\Sigma\, q_ia_i = 1, \qquad i = 1, 2, \ldots, n.$$

Our next theorem establishes the equivalence of these definitions.

Theorem 2.1. Let R be an integral domain. A non-zero ideal I of R is projective if and only if I is invertible.

Before we prove this we need the dual basis lemma.

Lemma 2.2. Let R be any ring and M a left R-module. M is projective if and only if there exists a family $\{x_i\}$, $i \in A$, of elements of M and a family $\{u_i\}$, $i \in A$, of elements of

$$M^* = \mathrm{Hom}_R\,(M, R)$$

such that

i) for $x \in M$, $u_i(x) = 0$ for all but a finite number of the i's, and

ii) for $x \in M$, $x = \sum_i u_i(x)x_i$.

PROOF: If M is projective with generators $\{x_i\}$, $i \in \Lambda$, define F, a free module with base $\{X_i\}$, where i ranges over the same index set Λ, and further define

$$\pi : F \to M$$

by

$$\pi(X_i) = x_i,$$

extending by linearity. M is a direct summand of F since it is projective; hence, it can be considered as a submodule of F. If $x \in M$, $x = \sum_i a_i X_i$ and the a_i's are well-defined functions of x; indeed, the maps

$$u_i : M \to R$$

given by

$$u_i(x) = a_i, \qquad i \in \Lambda$$

are R-homomorphisms, i.e., $u_i \in M^*$. Now if $x \in M$ then

$$\pi x = x = \Sigma\, a_i x_i = \Sigma\, u_i(x) x_i.$$

Since $M \subset F$, which is a direct sum of copies of R, we see that the condition that $u_i x$ is 0 for all but a finite number of the i's is satisfied.

Conversely, given the $x_i \in M$ and $u_i \in M^*$, $i \in \Lambda$, we form the free module F as above and define a map

$$\pi : F \to M$$

via

$$\pi(X_i) = x_i$$

and extend by linearity. Clearly π is an epimorphism. We now define a map

$$\phi : M \to F$$

such that

$$M \xrightarrow{\phi} F \xrightarrow{\pi} M$$

is the identity on M. This is done by setting, for

$$x = \Sigma\, u_i(x)x_i,$$

where $x_i \in M$,

$$\phi(x) = \Sigma\, u_i(x)X_i.$$

This is clearly a homomorphism of F and $\phi\pi = 1_M$; hence M is a direct summand of F and therefore projective. We note also that $\{x_i\}$ is a generating set for M.

PROOF of Theorem 2.1: Assume I is invertible and define

$$\phi_i(x) = q_i x$$

for $x \in I$ and $q_i \in K$, $q_i \neq 0$, the field of quotients of R. Then

$$\phi_i \in \mathrm{Hom}_R\,(I, R) = I^*$$

and

$$\Sigma\, \phi_i(x)a_i = \Sigma\, q_i x a_i = x\, \Sigma\, q_i a_i = x$$

where $a_i \in I$. Then by the lemma, I is projective.

Assume now that I is projective and let $\{x_i\}$ and $\{u_i\}$ be as in the lemma. Then for each $i \in \Lambda$ we have

$$xu_i(y) = u_i(xy) = yu_i(x)$$

for $x, y \in I$. Thus $q_i = u_i(x)/x$ for each x in I, $x \neq 0$, is an element of the quotient field such that $u_i(y) = q_i y$ for all y in I. It follows that $q_i I \in R$. If $x \neq 0$ then $u_i(x) = q_i x$ is zero for all but a finite number of indices. It then follows that all q_i excepting a finite number are zero, since R is an integral domain.

Condition (2) of the lemma gives

$$x = \Sigma_i u_i(x)x_i = \Sigma_i (q_i x)x_i = (\Sigma_i q_i x_i)x$$

which says that $\Sigma q_i x_i = 1$. Thus I is invertible.

Lemma 2.3. Let I be an ideal of R, a Dedekind ring, and M a finitely generated R-module such that $IM = M$. Then there exists an element $a \in I$ such that $(1 - a)M = 0$.

PROOF: I is finitely generated. Let x_i, $i = 1, 2, \ldots, n$, be a generating set for M. Since $M = IM$ we have relations of the form;

$$x_i = \Sigma y_{ij} x_j, \qquad y_{ij} \in I, \qquad \text{where } i = 1, 2, \ldots, n.$$

or

$$(\delta_{ij} - y_{ij})x_j = 0$$

where

$$\delta_{ij} = 0 \qquad \text{if } i \neq j \text{ and } \delta_{jj} = 1.$$

If Δ is the determinant $|\delta_{ij} - y_{ij}|$, the argument leading to Cramer's rule shows $\Delta x_j = 0$ for all j; that is, $\Delta M = 0$. Δ is of the form $1 - y$ where $y \in I$.

If A is a submodule of B we denote by $A : B$ the set $\{r \in R \mid rB \subset A\}$.

Lemma 2.4. Let A be a submodule of B where B is a finitely generated R-module. Let I be an arbitrary ideal of R. The following statements are equivalent:

1) $A/IA \to B/IB$ is an isomorphism.

2) $A/IA \to B/IB$ is an epimorphism.

3) $I(B/A) = B/A$.

4) $I + A{:}B = R$, that is, I is prime to $A{:}B$.

PROOF: We show first that (2) implies (3). From (2) we see that any element of B is congruent mod (IB) to an element of A. Therefore, $B = A + IB$. This clearly implies (3). We now show that (3) implies (4). By Lemma 2.3, there exists an $a \in I$ such that

$$(1 - a)B/A = 0,$$

that is,

$$(1 - a) \in A:B.$$

Since $a + (1 - a) = 1$, $I + A:B = R$. Suppose that (4) holds. Then we have that

$$B = IB + A,$$

since clearly $B \supseteq IB + A$, and

$$B = (I + A:B)B = IB + (A:B)B \subset IB + A.$$

Further,

$$IB \cap A = IA$$

since the quotient

$$(IB \cap A)/IA$$

is annihilated by both I and $A:B$, hence by R. Now, by the Fundamental Theorem of Homomorphisms we have

$$B/IB = (IB + A)/IB \cong A/(IB \cap A) = A/IA.$$

Lemma 2.5. Let R be a commutative ring with identity. Let F be an RH-module which is a free R-module. Then $RH \otimes F$ is a RH-free module.

PROOF: As a R-module, $RH \otimes F$ is a direct sum

$$\oplus\, Rx \otimes F$$

taken over all $x \in H$. Let $\{e_\alpha\}$ be a R-base for F. If $x \in H$, $\{xe_\alpha\}$

is easily seen to be a R-base for F, since if

$$\sum_{i=1}^{n} a_i x e_{\alpha_i} = 0 \qquad \text{where } a_i \in R$$

then

$$x \sum_{i=1}^{n} a_i e_{\alpha i} = 0$$

and necessarily $a_1 = a_2 = \cdots = a_n = 0$. Now we have that $\{x \otimes xe_\alpha\}$ is a RH-base for $RH \otimes F$ which implies that $\{1 \otimes e_\alpha\}$ is a RH-base for $RH \otimes F$.

Theorem 2.6. Let R be a commutative ring with identity. Let A and P be RH-modules such that P is RH-projective and A is projective as a R-module. Then $A \otimes P$ is a projective RH-module.

PROOF: If A is R-free and P is RH-free, we are done by Lemma 2.5, since P is isomorphic to a direct sum of copies of RH. If A is RH-free, choose a projective RH-module P' such that $P \oplus P'$ is RH-free. Then $(A \otimes P) \oplus (A \otimes P')$ is free and $A \otimes P$ is projective. In the general case, let A' be a R-module such that $A \oplus A'$ is R-free. Make A' into a RH-module by having H act trivially on A'. Then $(A \otimes P) \oplus (A' \otimes P) \cong (A \oplus A') \otimes P$ is projective. Therefore $A \otimes P$ is projective as a direct summand of a projective module.

We must digress from the topic at hand to examine an extension of a Dedekind ring. Let R be a Dedekind ring and P a proper ideal of R. We form R - P, the complement of P in R when viewed as sets. R - P is multiplicatively closed and contains no zero divisors. We define the set of <u>formal quotients</u>--a/c--where $a \in R$, $c \in R - P$. We define addition and multiplication in a manner analogous to the procedure followed in defining the rational numbers. This procedure yields a ring, denoted R_p, which we will call the ring of quotients of R formed with respect to P. We see that R_p is a local ring, since it has only one maximal ideal R_pP.

Let L be an arbitrary local ring with maximal ideal $\mathfrak{M}$. Let $b_1, b_2, \ldots$ be an infinite sequence of elements of R, and let $b \in R$. We shall say the sequence $[b_n]$ converges to b, denoted $b_n \to b$ as $n \to \infty$ or simply $b_n \to b$, in case the following condition is satisfied:

Given any integer $s \geq 0$, there exists an integer N such that

$$b - b_n \in \mathfrak{M}^s \text{ for all } n > N.$$

The operations of addition, subtraction and multiplication are "continuous" operations, as can be readily verified.

We further define a Cauchy sequence as a sequence $[a_n]$ with the property that given any $s \geq 0$ there exists an integer N such that $a_n - a_m \in \mathfrak{M}^s$ whenever $n > m > N$.

We say a local ring is complete if every Cauchy sequence converges to a point in the local ring. This is analogous to the property of being complete in the field of real numbers.

Let L be a local ring. A local ring $\overline{L}$ is called a completion of L in case

1) A sequence of elements of L is a Cauchy sequence if and only if it is a Cauchy sequence in $\overline{L}$,

2) $\overline{L}$ is complete and

3) Every element of $\overline{L}$ is the limit of a sequence of elements of L.

It is well known that every local ring has a completion [5].

Lemma 2.7. Let R be a Dedekind ring with prime ideal P. Let L be the completion of R_P, and $\overline{P}$ its maximal ideal. Then $R/P \cong L/\overline{P}$.

PROOF: We have the natural homomorphism

$$L \to L/\overline{P}.$$

This will induce a homomorphism on R which will have

$$\overline{P} \cap R = P$$

as kernel.

We will require the well-known Chinese Remainder Theorem which we here state without proof.

Theorem (Chinese Remainder) [7]. A Dedekind ring R possesses the following property:

Given a finite number of ideals P_i and of elements x_i of R, $i = 1, 2, \ldots, n$, the system of congruences $x \equiv x_i \pmod{P_i}$ admits a solution x if and only if we have $x_i \equiv x_j \pmod{P_i + P_j}$ for $i \neq j$.

Theorem 2.8. Let R be a Dedekind ring, K its field of quotients and H a finite group. Let M be a projective RH-module such that $K \times M$ is KH-free and let I be any non-zero ideal in R. Then there exists a free RH-module $F \subset M$ such that

$$I + (F:M) = R.$$

PROOF: If $I = R$ then any free RH-module $F \subset M$ would suffice. (There exists one by Theorem 0.3.) So we may assume that $I \neq R$. Let $I = P$ be a prime ideal. Let L be the completion of R_P, the ring of quotients. Let $\overline{P}$ be the maximal ideal of L and $\overline{K}$ the quotient field of L. $K \subset \overline{K}$, clearly. By Lemma 2.7 $R/P \cong L/\overline{P}$.

Let $\overline{M} = L \otimes_R M$. Then

$$\overline{K} \otimes_L \overline{M} \cong \overline{K} \otimes_L L \otimes_R M \cong \overline{K} \otimes_R M \cong \overline{K} \otimes_K K \otimes_R M$$

is $\overline{K}H$-free, since $K \otimes_R M$ is KH-free. By Theorem A then

$$\overline{M} = L \otimes_R M$$

is LH-free. Therefore

$$M/PM \cong R/P \otimes_R M \cong L/\overline{P} \otimes_L L \otimes_R M \cong L/\overline{P} \otimes_L \overline{M}$$

is free over

$$(L/\overline{P})H = (R/P)H$$

by application of Lemma 2.6, with H the trivial group.

R is a Dedekind domain and we can factor an ideal into prime ideals in any Dedekind domain. Let $I = \prod_{i=1}^{k} P_i$ where the P_i's are distinct prime ideals. Then for each i, $1 \leq i \leq k$, there exist elements $m_{1i}, \ldots, m_{qi} \in M$ such that

$$M/P_iM = \bigoplus_{j=1}^{q} (R/P_i)Hm_{ji}$$

because, M/P_iM being $(R/P_i)H$-free, it is a direct sum of copies of $(R/P_i)H$. Note that $q[H:1]$ = R-rank of M = $(K \otimes M : K)$ since

$$\begin{aligned} K \otimes_R M &\cong K \otimes_R R/P_i \otimes_{R/P_i} M \\ &\cong K \otimes_R \left(\bigoplus_{j=1}^{q} (R/P_i)Hm_{ji} \right. \\ &\cong \bigoplus_{j=1}^{q} K \otimes_R (R/P_i)Hm_{ji} \cong \bigoplus_{j=1}^{q} KHm_{ji}. \end{aligned}$$

This then shows that q is independent of the P_i chosen.

By the Chinese Remainder Theorem we can choose $\alpha_1, \ldots,$ $\alpha_k \in R$ such that

$\alpha_i \equiv 1 \bmod P_i$, and

$\alpha_i \equiv 0 \bmod P_j$, $\qquad j \neq i,\ 1 \leq i,\ j \leq k.$

Let

$$x_j = \alpha_1 m_{j1} + \cdots + \alpha_k m_{jk}, \qquad 1 \le j \le q$$

and

$$F = RHx_1 + RHx_2 + \cdots + RHx_q.$$

Now, F is an RH-submodule of M which is RH-free since any non-trivial relation

$$\Sigma \alpha_{ij} r_j x_i = 0; \qquad \{\alpha_{ij}\} \in R,\ \{r_j\} \in H,\ 1 \le i \le k,\ 1 \le j \le q$$

would continue to hold in $K \otimes F$ and hence,

$$(K \otimes F : K) < q[H:1]$$

which we will show is a contradiction.

By construction,

$$F \otimes R/P \cong M \otimes R/P$$

via

$$\phi\left(\bigoplus_{j=1}^{q} RH\alpha_i m_{ji}\right) = \bigoplus_{j=1}^{q} R/P\, Hm_{ji}, \text{ for } P \text{ dividing } I.$$

By Lemma 2.4 we have

$$P + (F:M) = R$$

for each P dividing I.

Assume

$$P_1 + (F:M) = R \qquad \text{and} \qquad P_2 + (F:M) = R.$$

Then

$$a_1 + b_1 = 1 \text{ and } a_2 + b_2 = 1,$$

where

$$a_1 \in P_1, \quad a_2 \in P_2 \qquad \text{and} \qquad b_1, b_2 \in (F:M).$$

Then

$$a_1 a_2 + a_1 b_2 + a_2 b_1 + b_1 b_2 = 1,$$

where

$$a_1a_2 \in P_1 \quad \text{and} \quad a_1b_2 + a_2b_1 + b_1b_2 \in (F:M).$$

Therefore we have

$$I + (F:M) = R.$$

Corollary 2.9. Let M be a projective finitely generated RH-module and I any ideal of R, a Dedekind ring. Then there exists a RH-free module F' containing M such that

$$I + (M:F') = R.$$

PROOF: We may assume $I \neq R$. Let F be the free module constructed in the theorem so that $I + (F:M) = R$. Then there exists $\alpha \in I$ and $\beta \in F:M$ such that $\alpha + \beta = 1$. Now $\beta \neq 0$ and $M \cong \beta M$, since M necessarily is torsion-free. Now $\beta M \subset F$ and $\beta \in \beta M:F$. Since $\alpha + \beta = 1$,

$$I + (\beta M:F) = R.$$

We will again digress to pick up some terminology and properties which will facilitate matters. By a <u>projective resolution</u> of a R-module A we will mean an exact sequence

$$\cdots \to P_2 \to P_1 \to P_o \to A \to 0$$

with each P_i projective. In Chapter 0 we showed that each module is a homomorphic image of a R-free (hence, projective) module. Consequently, given A we can always construct a free (projective) resolution. We say that A has <u>projective dimension</u> n in case:

1) There exists an exact sequence of the form

$$0 \to P_n \to \cdots \to P_1 \to P_o \to A \to 0$$

where each P_i is R-projective and

2) There exists no sequence of this type with a smaller number of terms.

Conversely, let us note that if A is projective then the sequence

$$0 \to A \xrightarrow{1_A} A \to 0,$$

where 1_A is the identity map is such a sequence; hence, A has projective dimension 0, or PdA = 0.

Lemma 2.10. Let I be a left ideal in R such that

$$[H:1]R + I:RH = R.$$

Then I is projective.

PROOF: Let M = RH/I. By the hypothesis we can find b ε I:RH, a ε R such that

$$[H:1]a + b = 1.$$

Note that bM = 0. Define Θ:M $\to$ M by

$$\Theta(x) = ax \quad \text{for} \quad x \in M.$$

Now we have that

$$\sum_{g \in H} g\Theta(g^{-1}x) = \sum_{g \in H} gag^{-1}x = [H:1]ax = [H:1]ax + bx = x.$$

We next show that M is a direct summand of RH $\otimes$ M. Define

$$f(g, x) = g\Theta(g^{-1}x), \qquad \text{for } g \in H \text{ and } x \in M.$$

Further, define

$$v(x) = \Sigma\, g \otimes f(g, x).$$

We have a map

$$f':RH \otimes M \to M \qquad \text{by } f(g \otimes x) = x.$$

Consider the diagram

$$M \xrightarrow{v} RH \otimes M \xrightarrow{f'} M.$$

Now, if $x \in M$,

$$f'v(x) = f'(\Sigma\, g \otimes f(g, x))$$

$$= \Sigma\, f(g, x) = \Sigma\, g0(g^{-1}x) = x.$$

By Proposition 0.1, M is a direct summand of $RH \otimes M$. Therefore it is sufficient to show that $RH \otimes M$ has projective dimension ≤ 1. Let

$$0 \to A \to P \to M \to 0$$

be exact with A and P torsion free. Then

$$0 \to RH \otimes A \to RH \otimes P \to RH \otimes M \to 0$$

is exact. $RH \otimes A$ and $RH \otimes P$ are projective by Theorem 2.6 so $RH \otimes M$ has projective dimension ≤ 1. But,

$$0 \to I \to RH \to M \to 0$$

is a resolution of M so I is projective, since RH is projective over R.

Lemma 2.11. Let R be a Dedekind domain and K its field of quotients. Let M be a projective finitely generated RH-module such that $K \otimes M$ is KH-free and let I be a non-zero ideal in R. Then there exists a finite set of left ideals $\{M_i\}$ $(i = 1, 2, \ldots, k)$ of RH, which are projective RH-modules, satisfying

$$I + M_i{:}RH = R \qquad \text{for each } i$$

and such that

$$M = \oplus\, M_i, \qquad i = 1, 2, \ldots, k.$$

PROOF: By Corollary 2.9 there exists a free RH-module F' containing M such that

$$[H{:}1]I + M{:}F' = R.$$

Let F' be a direct sum of k copies of RH, and let

$$\Theta : F' \to RH$$

be the projection of F' onto the first summand. Θ maps M onto a left ideal M_1 of RH. If $\alpha F' \subset M$ for $\alpha \in RH$ then $\alpha RH \subset M_1$ so that

$$M:F' \subset M_1:RH.$$

Therefore,

$$[H:1]I + M_1:RH = R,$$

so that

$$[H:1]R + M_1:RH = R, \qquad I + M_1:RH = R.$$

The first equation implies that M_1 is projective, by Lemma 2.10.

We may write the exact sequence

$$0 \to N \to M \xrightarrow{\Theta} M_1 \to 0$$

where N is ker Θ. Since M_1 is projective,

$$M \cong M_1 \oplus N$$

and N is projective. Now we may repeat the argument on N. We now note that the process must cease since the R-rank of N is less than the R-rank of M.

Now we are in a position to prove the main result of Swan.

Theorem 2.12. Let R be a Dedekind domain and its field of quotients. Let M be a projective finitely generated RH-module such that $K \otimes M$ is KH-free and let I be a non-zero ideal in R. Then there exist a free RH-module F and a projective left ideal M_0 of RH such that

$$M \cong F \oplus M_0 \qquad \text{and} \qquad I + M_0:RH = R.$$

PROOF: In view of the preceding lemma, it will suffice to show that if M_1 and M_2 are projective ideals in RH such that

$$I + M_i:RH = R \qquad i = 1, 2$$

then there exists a projective ideal M_3 in RH such that

$$I + M_3:RH = R \text{ and } M_1 \oplus M_2 = RH \oplus M_3.$$

Let $J = M_1:RH$. By Lemma 2.11, there exists a finite number of ideals $\{N_i\}$ of RH which are projective RH-modules satisfying

$$IJ + N_i:RH = R$$

such that

$$M \cong \bigoplus_i N_i.$$

M is finitely generated so we can apply the Krull-Schmidt Theorem which says that if

$$M \cong \bigoplus_{i=1}^{n} M_i = \bigoplus_{j=1}^{k} M_j$$

where M_i and M_j are indecomposable (cannot be written as a direct sum) then $n = k$ and the decomposition is unique up to order

Therefore, we have that there exists an ideal M_2' in RH such that

$$IJ + M_2':RH = R \qquad \text{and} \qquad M_2' \cong M_2.$$

Now

$$M_1 \oplus M_2' \cong M_1 \oplus M_2,$$

and we can choose

$$\alpha \in M_1:RH, \qquad \beta \in M_2':RH$$

such that $\alpha + \beta = 1$, because $IJ \leq M_1:RH$.

Let $\{e_1, e_2\}$ be a RH-basis for a free module F defined by

$$F = RHe_1 \oplus RHe_2.$$

Then we define

$$N = M_1e_1 \oplus M_2'e_2 \cong M_1 \oplus M_2.$$

and we have, after some elementary computations, that

$$I(N/F) = N/F.$$

Thus $N:F + I = R$, by Lemma 2.4.

Set $e_1' = \alpha e_1 + \beta e_2$, $e_2' = e_1 - e_2$. Then $\{e_1', e_2'\}$ is also a free RH-base for F, since

$$e_1 = e_1' + \beta e_2'$$

and

$$e_2 = e_1' - \beta_2 e_2'.$$

Since $\alpha \in M_1$, (because $\alpha RH \subset M_1$), and $\beta \in M_2'$ we have that $e_1' \in N$.

Hence

$$N = RHe_1' + M_3 e_2$$

where

$$M_3 = \{x \in RH | xe_2' \in N\}.$$

M_3 is clearly an ideal in RH for which $M_1 \oplus M_2' \cong N \cong RH \oplus M_3$.

Also,

$$M_3 : RH = N : F$$

so

$$I + N:F = I + M_3:RH = R.$$

CHAPTER III.

WHEN IS K $\otimes$ M KH-FREE?

Throughout Chapter Two we required that K x M be KH-free in many of the theorems. The natural question to ask is "When does this occur?" If H is the trivial group then K $\otimes$ M is KH-free, since it is a vector space.

Swan gives an elegant theorem which does give a less trivial condition:

Theorem. Let R be a Dedekind ring of characteristic zero. Let H be a finite group with order [H:1]. Assume no rational prime dividing [H:1] is a unit in R. Then if M is any finitely generated projective RH-module, K $\otimes$ M is KH-free.

The proof is omitted since, as in Theorem A, it would require a deep knowledge of group characters.

Swan's Theorem (2.12) shows that a projective RH-module is not too far removed from being a free RH-module, and in fact is of the form F $\oplus$ M_o, where F is free and M_o is a projective left ideal in RH. Concerning such an ideal M_o, we know that for each prime ideal P in R, the module M_o/PM_o is free as a (R/P)H-module. Furthermore, we know K $\otimes$ M_o $\cong$ KH. The Jordan-Zassenhaus Theorem [2; 79.1] states that there are only a finite number of non-isomorphic RH-modules M_i such that

$$K \otimes M_i \cong KH,$$

and thus there exist a finite number of projective left ideals M_i of RH such that every projective RH-module is of the form $F \oplus M_i$ for some free module F and some i.

LIST OF REFERENCES

1. H. Cartan and S. Eilenberg, Homological Algebra, Princeton, 1956.

2. C. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience Publishers, New York, 1962.

3. I. Kaplansky, Projective Modules, Ann. of Math., 68(1958), 372-377.

4. D. G. Northcott, Ideal Theory, Cambridge Tracts No. 42, 1953.

5. D. G. Northcott, Introduction to Homological Algebra, Cambridge Press, Cambridge, England, 1960.

6. R. G. Swan, Induced Representations and Projective Modules, Ann. of Math., 71(1960, 552-578.

7. O. Zariski and P. Samuel, Commutative Algebra, Vol. I, van Nostrand Co., Princeton, 1958.